WHITE PAPER

Layers of Industrial Control System Security

OT Cybersecurity for the Modern Threat Landscape

FOUNDATIONAL CONTROLS FOR
SECURITY, COMPLIANCE & IT OPERATIONS

An Extremely Brief History of ICS Security

Industrial control systems (ICS) proliferated before cybersecurity became the mission-critical concern it is today. The shift to new network technologies improves data collection, efficiency and time-to-market, but it also produces new cybersecurity risks:

> 69% of respondents to a 2017 SANS ICS survey consider the threat to their systems as "severe."

- Many ICS are purpose-built and proprietary, making them out of sync with modern cybersecurity standards.
- Legacy ICS are flat, meaning each device has access to the rest. In a flat system, a malware attack against one device gives cybercriminals free reign over the entire network.
- ICS are now increasingly enmeshed with IT business infrastructure and devices, multiplying the risk of their command and control functions being compromised by cyber adversaries.

Network Segmentation

Network segmentation is the first answer to insufficient ICS cybersecurity. You'll also need strategies for asset discovery, vulnerability assessment and continuous monitoring.

Network segmentation means placing host devices into a subnet zone where they share common operational and security requirements. If one host—like a programmable logic controller (PLC)—gets compromised, it can only affect other hosts within the same zone.

Network segmentation quarantines attacks to the zone they hit, protecting the rest of your network from further damage. Let's take a deeper look at how network segmentation works.

Zones and conduits

Segmentation is achieved by dividing your network into zones and conduits. The International Society for Automation and International Electrotechnical Commission (ISA/IEC) 62443 ICS security standard introduced the concept of segmentation using a zone and conduit framework.

- A zone is a grouping of logical or physical assets that share common security requirements based on factors like criticality and consequence.
- Conduits control access to zones, resist Denial of Service (DoS) attacks and the transfer of malware, shield other network systems and protect the integrity and confidentiality of network traffic.

Tip: Focusing on Focusing on monitoring and protecting conduits is typically far more cost-effective than having to upgrade every device or computer in a zone to meet a requirement.

Defense in depth

Network segmentation and zones and conduits go hand-in-hand with using industrial firewalls to help achieve what's called "defense in depth," a proven strategy you can use to secure your networks.

Asset Discovery

How can you secure what you don't know you have? Maintaining an accurate hardware, firmware and software inventory is paramount if you want to protect your systems from cyber attacks. The inventory of components that make up your control system must also be updated over time as new assets are added or retired.

Initiate asset inventory by inspecting your network to identify what's connected to it. Passive asset discovery solutions are essential, as they provide accurate network topology without impacting operations within traffic-sensitive OT environments. Active scanning can disrupt an asset, impeding productivity and revenue.

Tripwire Log Center

Tripwire® Log Center® is a powerful aggregation tool with built-in intelligence that inspects logs for devices and IP addresses. Tripwire Log Center helps you get started quickly with security solution packs for the following situations:

- Insider threats
- Breach detection
- DDoS detection
- Authentication
- User Audits
- Intrusion detection

Tripwire Log Center gives you granular asset discovery on an ICS scale. It does so without interfering with plant performance, unlike other asset discovery solutions on the market. Here are just a few ways Tripwire Log Center is equipped to handle even the most complex ICS OT environments:

- **Passive asset discovery:** It identifies previously unknown assets for future monitoring.
- **Tool integration:** It Integrates with Tofino to monitor multiple Tofino firewalls via a single dashboard
- **It's at home in ICS:** Tripwire Log Center follows normalization and correlation rules for many industrial devices.

Vulnerability Assessment

Attacks on ICS grow more inventive by the day, so you need to take an aggressive, proactive approach to outpace them. Once you've segmented your network and you know what's on it, you can start discovering, prioritizing and managing the vulnerabilities on it.

Vulnerabilities can stem from ICS components, third-party hardware and software, industrial routers and IoT devices. Vulnerabilities from both hardware and software systems often go undetected, providing an easy entry point for hackers.

Vulnerability assessment challenges

What would it cost you if your ICS network went down for an hour? What about an entire day? Proactive vulnerability assessment can keep that from happening by giving you total visibility into your operational technology (OT) environments.

Unauthorized configuration changes, whether accidental or intentional, can cripple plant operations systems. And changes that affect the secure or hardened configuration of a device can leave it vulnerable to malware and malicious behavior that can quickly negatively impact your ICS.

You need the ability to analyze your ICS for configuration security and run policy tests against best practices and compliance standards like IEC 62443. However, legacy protocols that aren't supported by modern security vendors can impede accurate vulnerability assessment.

Tripwire Enterprise with Tripwire Data Collector

Tripwire Data Collector is a feature of Tripwire Enterprise that helps you securely configure your assets by scanning your network for devices and bringing them into your inventory.

Tripwire Data Collector benefits:

» Speaks to legacy native industrial protocols like Modbus TCP, Ethernet IP CIP and SNMP

» Integrations with Rockwell AssetCentre, MDT AutoSave and Kepware

» Reduces manual effort to summarize policy and compliance efforts

» Reduces downtime of ICS networks by quickly alerting for unwanted change

» "No touch" approach won't disrupt devices

» Vulnerability risk scoring

Continuous Monitoring

The last decade saw the convergence of IT/OT and ICS. The adoption of more IT systems into ICS environments puts industrial control networks at greater risk. That's why continuous monitoring of hardware and software changes is absolutely necessary for securing plants.

> Cyber attacks typically exploit known vulnerabilities by injecting malware. A 2017 report found that 40 percent of all energy-sector ICS were attacked by malware at least once, with major other ICS industries following close behind.

Every incident begins with a detectable change

ICS devices produce logs containing information about activities on components, potential faults around operational disruption, and security events like unsuccessful logins. Not monitoring this information can leave you blind to potential operational and cybersecurity events.

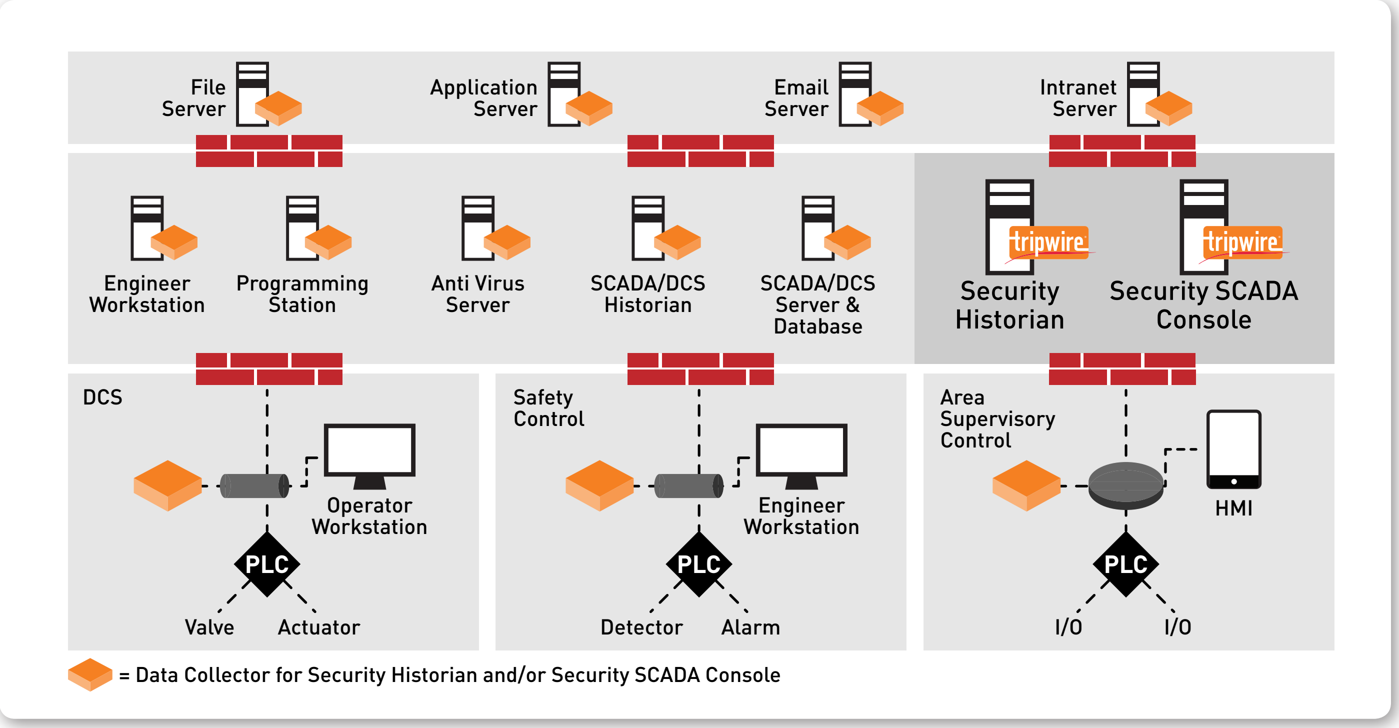

Fig. 1 Tripwire's flexible data collection works throughout your network to help ensure availability, security and resilience

Without monitoring tools, responding to malware is extremely difficult. If you can't ascertain what systems and applications are impacted by malware, you can lose substantial time and resources trying to return to cyber integrity after an attack.

Meeting and maintaining regulatory compliance

Regulatory compliance standards require monitoring solutions to automate the collection of evidence for the implementation of cybersecurity controls.

- IEC 62443 is an ICS compliance standard that makes recommendations on network architecture, configuration, and monitoring.
- The National Institute of Standards Technology's NIST 800-53 is a government-supplied catalog of cybersecurity best practices.
- The International Standards Organization (ISO) provides another set of general guidelines to be followed for optimized security, the ISO 27001.
- Tripwire Enterprise measures how systems/devices are configured against the recommendations made by these standards, and alerts you about deviations from these best practices within your ICS.

Tripwire Enterprise: Advanced ICS Monitoring

All modern ICS needs continuous monitoring, and Tripwire Enterprise is available to do the heavy lifting. Tripwire Enterprise helps you achieve superior system hardening and reduce your attack surface through continuous change monitoring. Be the first to know about changes within your operating systems and network configurations, and monitor open ports and services.

The Tripwire ICS Security Suite

The Tripwire ICS Security Suite comes from the most trusted name in cybersecurity. The suite includes Tripwire Enterprise (with Tripwire Data Collector) and Tripwire Log Center. Here are a few common ICS security problems and how it addresses them:

Issue	Impact	Solution
No visibility into vulnerable hardware and software that could be exploited to damage or shut down plant operations	Cyberattacks typically exploit known vulnerabilities to inject malware that damages target systems	Continuous assessment of hardware and software vulnerabilities that need to be addressed
Intrusive security tools that could adversely impact plant performance	Standard security approaches that actively scan networks can take them down	Unique no-touch approach to identify and report on potential weaknesses
No monitoring of hardware and software changes that could adversely impact plant performance	Unauthorized configuration changes, whether accidental or intentional, can cripple plant operations systems	Change data collection via passive (device syslog) or active (real-time monitoring) approach to support incident investigation
Manual efforts to collect and summarize proof of compliance with regulatory requirements	Extra work required from plant operations and compliance teams reduces productivity	Automated data collection, and predefined alerts and reporting aligned to industry regulations or standards (e.g. NERC CIP, IEC 62443, NIST 800-53)

Fig. 2 How the Tripwire ICS Security Suite addresses common ICS security issues

Request a Demo

Let us take you through a demo of the Tripwire ICS Security Suite and answer any questions you have. Understand how Tripwire's suite of security and vulnerability management products and services can be customized to your specific OT security and compliance needs. Visit here to schedule your demo.

The Tripwire ICS Security Suite integrates with a number of industry-leading solutions to offer you the most robust framework possible to mitigate ICS cyber threats.

Summary

Tripwire solutions provide the security your ICS requires to thrive in today's threat landscape. Put layered ICS security best practices to work for you with Tripwire Log Center, Tripwire Enterprise and Tripwire Data Collector. When your OT environment's security system is running smoothly, you can put your focus where you want it: on safety, quality and productivity.

Tripwire is the trusted leader for establishing a strong cybersecurity foundation. Partnering with Fortune 500 enterprises, industrial organizations and government agencies, Tripwire protects the integrity of mission-critical systems spanning physical, virtual, cloud and DevOps environments. Tripwire's award-winning portfolio delivers top critical security controls, including asset discovery, secure configuration management, vulnerability management and log management. As the pioneers of file integrity monitoring (FIM), Tripwire's expertise is built on a 20+ year history of innovation helping organizations discover, minimize and monitor their attack surfaces. **Learn more at tripwire.com**

***The State of Security*: Security news, trends and insights at tripwire.com/blog**
Connect with us on LinkedIn, Twitter and Facebook